Discrete Applied Mathematics 157 (2009) 428–432

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Note

On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2

Hyeonjin Kim [a,b,*], Sung-Mo Park [b], Sang Geun Hahn [a]

[a] Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology, 373-1 Guseong-Dong, Daejeon 305-701, South Korea

[b] The Attached Institute of ETRI, 909 Jeonmin-Dong, Daejeon 305-390, South Korea

ARTICLE INFO

Article history:
Received 6 December 2007
Received in revised form 16 May 2008
Accepted 21 June 2008
Available online 3 August 2008

Keywords:
Boolean function
Rotation symmetric
Hamming weight
Nonlinearity

ABSTRACT

We improve parts of the results of [T. W. Cusick, P. Stanica, Fast evaluation, weights and nonlinearity of rotation-symmetric functions, Discrete Mathematics 258 (2002) 289–301; J. Pieprzyk, C. X. Qu, Fast hashing and rotation-symmetric functions, Journal of Universal Computer Science 5 (1) (1999) 20–31]. It is observed that the n-variable quadratic Boolean functions, $f_{n,s}(x) := \sum_{i=1}^{n} x_i x_{i+s-1}$ for $2 \leq s \leq \lceil \frac{n}{2} \rceil$, which are homogeneous rotation symmetric, may not be affinely equivalent for fixed n and different choices of s. We show that their weights and nonlinearity are exactly characterized by the cyclic subgroup $\langle s-1 \rangle$ of $\mathbb{Z}_n$. If $\frac{n}{\gcd(n,s-1)}$, the order of $s-1$, is even, the weight and nonlinearity are the same and given by $2^{n-1} - 2^{\frac{n}{2}+\gcd(n,s-1)-1}$. If the order is odd, it is balanced and nonlinearity is given by $2^{n-1} - 2^{\frac{n+\gcd(n,s-1)}{2}-1}$.

1. Introduction

The subject of Boolean functions is well established and constitutes a cornerstone of cryptography and coding theory. Recently, rotation symmetric Boolean functions have attracted attention due to their simplicity – invariant under rotation transform – for efficient computation. In [6], rotation symmetric functions are used for fast hash function design. The exact sizes of a few classes of rotation symmetric functions were computed in [7]. The size of whole space is roughly $2^{\frac{2^n}{n}}$, much smaller than the space of all Boolean functions. Utilizing the fact that Walsh transform of a rotation symmetric function is also rotation symmetric, several experimental searches were carried out in [3,7,8]. In particular, nine-variable functions having nonlinearity 241 were found in [3]. In another direction, on the basis of [5,9] and by experimental observation, a conjecture is given in [7] that there is no bent function of degree ≥ 3 which is homogeneous rotation symmetric.

In [6], the weight and nonlinearity of quadratic rotation symmetric functions were estimated and exactly formulated for some specific functions. In [2], more formulations for the exact values were carried out. By experiment, we observed that the results of [2,6] could be generalized naturally. Properties of second-order Reed–Muller codes given in [4] are revealed to be very useful for this purpose. We also found that the permutation associated with a quadratic function consisting of single orbit gives some important information for the function.

2. Notation and preliminaries

We denote an n-dimensional vector space over GF(2) by $\mathbf{V}_n$. There are 2^n vectors in $\mathbf{V}_n$. An n-variable Boolean function is a mapping from $\mathbf{V}_n$ to GF(2). The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. A Boolean function can be represented

* Corresponding author at: The Attached Institute of ETRI, 909 Jeonmin-Dong, Daejeon 305-390, South Korea. Tel.: +82 42 870 2124; fax: +82 42 870 2369.

E-mail addresses: mikjh@ensec.re.kr (H. Kim), smp@ensec.re.kr (S.-M. Park), sghahn@kaist.ac.kr (S.G. Hahn).

0166-218X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2008.06.022

as an algebraic form or as a truth table. Regarding the table form, $f(x) \in \mathcal{B}_n$ can be uniquely represented by a 2^n-bit string if we fix the ordering of x. An *algebraic degree* is the maximum number of variables contained in a term. Functions of degree at most 1 are called *affine* functions. The set of all affine functions in $\mathcal{B}_n$ is denoted by $\mathcal{A}_n$. We define the *weight* of a function by the number of $x \in \mathbf{V}_n$ such that $f(x) = 1$, denoted by $\mathrm{wt}(f)$. A function $f \in \mathcal{B}_n$ is *balanced* if $\mathrm{wt}(f) = 2^{n-1}$. The distance between two functions f and g, denoted by $d(f, g)$, is defined by $\mathrm{wt}(f+g)$, where the addition $f+g$ is taking place in GF(2). The set of all integers is denoted by $\mathbb{Z}$.

Definition 1. The *nonlinearity* of a function $f \in \mathcal{B}_n$ is the minimum distance between f and the set of all affine functions $\mathcal{A}_n$, and denoted by $\mathrm{NL}(f)$. That is, $\mathrm{NL}(f) = \min_{l \in \mathcal{A}_n} d(f, l)$.

Definition 2. Two functions $f, g \in \mathcal{B}_n$ are *affinely equivalent* if $g(x) = f(xA + b)$ for some nonsingular $n \times n$ matrix A over GF(2) and $b \in \mathbf{V}_n$. If f and g are affinely equivalent, we write them as $f \equiv g$.

It can be easily checked that weight and nonlinearity are invariant under nonsingular affine transforms. That is, if $f \equiv g$ then $\mathrm{wt}(f) = \mathrm{wt}(g)$ and $\mathrm{NL}(f) = \mathrm{NL}(g)$.

The following lemma is easy and can be found in [4]. It is known as the randomization lemma.

Lemma 3. *The weight of an n-variable function $f(x_1, \ldots, x_{n-1}) + x_n$ is 2^{n-1}.*

The following theorem, proved by Dickson, appears in [1]. A complete statement and proof can be found in [4].

Theorem 4. *Every function $f \in \mathcal{B}_n$ of degree 2 is affinely equivalent to one of the following three types: If f is balanced, it is equivalent to $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$ for some $k \leq \frac{n-1}{2}$. If f is not balanced, it is equivalent to $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + b$ for some $k \leq \frac{n}{2}$ and $b \in GF(2)$. If $\mathrm{wt}(f) < 2^{n-1}$ then $b = 0$. If $\mathrm{wt}(f) > 2^{n-1}$ then $b = 1$.*

Once a quadratic function is transformed to the equivalent function as in Theorem 4, there is a simple closed formula for its weight and nonlinearity. The following formula in Lemma 5 can be found in [4] and will be used here as a basic tool. We prove the lemma in a different way from [4].

Lemma 5. *Let $h(x) = \sum_{i=1}^{k} x_{2i-1}x_{2i} + \sum_{i=2k+1}^{n} a_i x_i$ be an n-variable function for $k \leq \frac{n}{2}$. Then the nonlinearity is given by $\mathrm{NL}(h) = 2^{n-1} - 2^{n-k-1}$. If all the linear terms vanish then its weight is the same as the nonlinearity; otherwise it is balanced.*

Proof. If there exist linear terms then $h(x)$ is balanced by Lemma 3.

We assume $a_{2k+1} = \cdots = a_n = 0$ and consider the weight of $h(x)$. The function $h(x)$ takes the value 1 exactly for $x \in \mathbf{V}_n$, at which the odd number of terms in the function takes the value 1. Hence the weight of $h(x)$ is given by

$$\left(\binom{k}{1}3^{k-1} + \binom{k}{3}3^{k-3} + \cdots + \binom{k}{k-1}3^1\right)2^{n-2k} \quad \text{if } k \text{ is even, and}$$
$$\left(\binom{k}{1}3^{k-1} + \binom{k}{3}3^{k-3} + \cdots + \binom{k}{k}3^0\right)2^{n-2k} \quad \text{otherwise.}$$

Using the binomial expansion of $(1+z)^k$ for $z = \pm 3$, we can see that the two expressions have the same closed formula $2^{n-1} - 2^{n-k-1}$.

Let $h_2(x)$ be the quadratic part of $h(x)$. By the definition of nonlinearity, $\mathrm{NL}(h) = \mathrm{NL}(h_2) = \min_{b,c} \mathrm{wt}(h_2(x) + b \cdot x + c)$ for $b = (b_1, \ldots, b_n) \in \mathbf{V}_n$, and $c \in \mathrm{GF}(2)$. Using new variables $u_i := x_i + b_i$ for $i = 1, \ldots, 2k$, and just renaming $x_{2k+1}, \ldots, x_n$ by $u_{2k+1}, \ldots, u_n$, we have an equivalent function of $h_2(x) + b \cdot x + c \equiv h_2(u) + \sum_{i=2k+1}^{n} b_i u_i + c'$ where $c' = \sum_{i=1}^{k} b_{2i-1}b_{2i} + c$ which is an independent parameter on GF(2). To get the minimum weight, in view of Lemma 3 and Theorem 4, we must have $b_{2k+1} = \cdots = b_n = c' = 0$. Hence, the nonlinearity of $h(x)$ is the same as the weight of its quadratic part. Therefore, $\mathrm{NL}(h) = 2^{n-1} - 2^{n-k-1}$. □

3. Previous results

First, we give a definition of rotation symmetric functions. Consider $\rho = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$, a permutation of rotation on $\{1, \ldots, n\}$. The permutation ρ gives rise to an *action* on $\mathbf{V}_n$ such that, for $x = (x_1, \ldots, x_n) \in \mathbf{V}_n$ and $k \in \mathbb{Z}$,

$$\rho^k(x) = (x_{\rho^k(1)}, \ldots, x_{\rho^k(n)}).$$

The indices can be written explicitly as, for $i = 1, \ldots, n$,

$$\rho^k(i) = \begin{cases} n & \text{if } i + k \equiv 0 \pmod{n}, \\ i + k \pmod{n} & \text{otherwise.} \end{cases} \tag{1}$$

The *orbit* of $x \in \mathbf{V}_n$ under ρ is the set $\{\rho^k(x) \mid k \in \mathbb{Z}\}$. Similarly, we can extend the action to a monomial $m(x) = x_{i_1} \cdots x_{i_d} \in \mathcal{B}_n$ by defining $\rho^k(m(x)) = x_{\rho^k(i_1)} \cdots x_{\rho^k(i_d)}$. We define the orbit of $m(x)$ similarly by $\{\rho^k(m(x)) \mid k \in \mathbb{Z}\}$.

Table 1
The weights and nonlinearity of $f_{n,s}$ for $6 \le n \le 16$ and $2 \le s \le \lceil \frac{n+1}{2} \rceil$

s	$n=6$		$n=7$		$n=8$		$n=9$		$n=10$		$n=11$		$n=12$		$n=13$		$n=14$		$n=15$		$n=16$	
	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL
2	24	24	64	56	112	112	256	240	480	480	1024	992	1984	1984	4096	4032	8064	8064	16384	16256	32512	32512
3	32	24	64	56	96	96	256	240	512	480	1024	992	1920	1920	4096	4032	8192	8064	16384	16256	32256	32256
4	28	bent	64	56	112	112	256	224	480	480	1024	992	1792	1792	4096	4032	8064	8064	16384	16128	32512	32512
5					120	bent	256	240	512	480	1024	992	2048	1920	4096	4032	8192	8064	16384	16256	32720	32720
6									496	bent	1024	992	1984	1984	4096	4032	8064	8064	16384	15872	32512	32512
7													2016	bent	4096	4032	8192	8064	16384	16128	32256	32256
8																	8128	bent	16384	16256	32512	32512
9																					32640	bent

For even n and $s = \frac{n}{2} + 1$, the function $f_{n,s}$ belongs to the class of Maiorana–McFarland bent functions.

Definition 6. A function $f \in \mathcal{B}_n$ is called *rotation symmetric* if $f(x) = f(\rho(x))$ for every $x \in \mathbf{V}_n$.

If a monomial $m(x)$ appears in a rotation symmetric function as a term then all monomials in the orbit of $m(x)$ should also appear in the function as terms. An example of a rotation symmetric function in $\mathcal{B}_4$ is $x_1x_3 + x_2x_4 + x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2$.

In [2,6], they focused primarily on the quadratic homogeneous rotation symmetric function consisting of a single orbit of a monomial x_1x_s, which is given by, for $2 \le s \le \lceil \frac{n}{2} \rceil$,

$$f_{n,s}(x) := x_1x_s + x_2x_{s+1} + \cdots + x_nx_{s-1}.$$

For even n and $s = \frac{n}{2} + 1$, it would be natural to define $f_{n,s}(x) := \sum_{i=1}^{\frac{n}{2}} x_ix_{i+\frac{n}{2}}$.

For when $s = 2$, bounds for the weight and nonlinearity of $f_{n,s}$ were given in [6] by

$$2^{n-2} \le \mathrm{wt}(f_{n,2}) \le 2^n + 2^{n-2} \quad \text{and} \quad \mathrm{NL}(f_{n,2}) \ge 2^{n-2}.$$

Moreover, when n is odd, the values are exactly formulated as

$$\mathrm{wt}(f_{n,2}) = 2^{n-1} \text{ (balanced)} \quad \text{and} \quad \mathrm{NL}(f_{n,2}) = 2^{n-1} - 2^{\frac{n-1}{2}}. \tag{2}$$

For the case of $s = 2$ and even n, the problem of deciding the exact values was settled in [2], with formulas being given by

$$\mathrm{wt}(f_{n,2}) = \mathrm{NL}(f_{n,2}) = 2^{n-1} - 2^{\frac{n}{2}}. \tag{3}$$

4. Experimental observation

In deriving the formulas (2) and (3), it is unclear whether they hold for the functions $f_{n,s}(x)$ for arbitrary s. Thus, using a computer program, we computed the weights and nonlinearities of $f_{n,s}$ for small values of n and s. The experimental results are shown in Table 1. One can see that, for fixed n, the weight and nonlinearity may vary with respect to s. This implies that they may not be affinely equivalent. Therefore, the results of [2,6] should be generalized.

5. Weight and nonlinearity of $f_{n,s}$

We start with the simpler case of $f_{n,s}$ for $s = 2$. The following Lemma 7 is a restatement of the results of [2,6] as given in (2) and (3). However, we give our own proof here which, we believe, is much more concise and consistent.

Lemma 7. *For even n, we have $f_{n,2} \equiv x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2}$ and $\mathrm{wt}(f_{n,2}) = \mathrm{NL}(f_{n,2}) = 2^{n-1} - 2^{\frac{n}{2}}$. For odd n, $f_{n,2} \equiv x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n$, and the function is balanced and $\mathrm{NL}(f_{n,2}) = 2^{n-1} - 2^{\frac{n-1}{2}}$.*

Proof. By rearranging terms of $f_{n,2}$ with respect to x_1, x_2, we have $f_{n,2} = (x_1+x_3)(x_2+x_n)+x_3x_4+x_4x_5+\cdots+x_{n-1}x_n+x_nx_3$. Using new variables $u_1 := x_1 + x_3$ and $u_2 := x_2 + x_n$, we have $f_{n,2} \equiv u_1u_2 + x_3x_4 + \cdots + x_nx_3$. Reducing all indices of x_i's by 2, we have $f_{n,2} \equiv u_1u_2 + f_{n-2,2}$. We can continue the same processes until we arrive at $f_{n,2} \equiv u_1u_2 + \cdots + u_{n-5}u_{n-4} + f_{4,2}$ for even n, and $f_{n,2} \equiv u_1u_2 + \cdots + u_{n-4}u_{n-3} + f_{3,2}$ for odd n. Since $f_{4,2} = (x_1 + x_3)(x_2 + x_4)$ and $f_{3,2} = (x_1 + x_3)(x_2 + x_3) + x_3$, we have the equivalent functions as stated in the lemma. For even n, applying Lemma 5 by taking $k = \frac{n-2}{2}$, we have $\mathrm{wt}(f_{n,2}) = \mathrm{NL}(f_{n,2}) = 2^{n-1} - 2^{\frac{n}{2}}$. For odd n, by Lemma 5, the function $f_{n,2}$ is balanced. By taking $k = \frac{n-1}{2}$, we have $\mathrm{NL}(f_{n,2}) = 2^{n-1} - 2^{\frac{n-1}{2}}$. □

Let ρ_s denote $\rho^{s-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ s & s+1 & \cdots & s-1 \end{pmatrix}$ for $2 \le s \le \lceil \frac{n}{2} \rceil$. If we see the representation of permutation ρ_s as a $2 \times n$ matrix, each column $\begin{pmatrix} i \\ \rho_s(i) \end{pmatrix}$ of the matrix ρ_s determines the term $x_i x_{\rho_s(i)}$ of $f_{n,s}(x)$. Therefore, the function $f_{n,s}$ can be represented by the permutation ρ_s and vice versa.

Considering ρ_s as an action on $\{1, \ldots, n\}$, the orbit of i under ρ_s is the set $\{\rho_s^k(i) \mid k \in \mathbb{Z}\}$. A permutation is called a *cycle* if it admits at most one orbit of size ≥ 2. The *length* of a cycle is the maximum size of its orbits. A cycle τ of length t is represented as $(i, \tau(i), \ldots, \tau^{t-1}(i))$. If we ignore the elements not moved by τ, the cycle τ uniquely determines the function $f_\tau := x_i x_{\tau(i)} + x_{\tau(i)} x_{\tau^2(i)} + \cdots + x_{\tau^{t-1}(i)} x_i$. The permutation ρ_s can be decomposed uniquely into disjoint cycles, $\rho_s = \tau_1 \cdots \tau_k$. Then we have $f_{n,s} = f_{\tau_1} + \cdots + f_{\tau_k}$.

We characterize the exact weight and nonlinearity of $f_{n,s}$ using the structure of the cycle decomposition of the associated permutation ρ_s.

Theorem 8. *Assume that the permutation ρ_s of the function $f_{n,s}$ has the disjoint cycle decomposition of $\rho_s = \tau_1 \cdots \tau_k$. Then, the number of cycles is $k = \gcd(n, s-1)$ and all the cycles have the same length of $\frac{n}{k}$. Furthermore, the weight and nonlinearity of $f_{n,s}$ are characterized as*

$$\mathrm{wt}(f_{n,s}) = \mathrm{NL}(f_{n,s}) = 2^{n-1} - 2^{\frac{n}{2}+k-1}, \quad \text{if } \frac{n}{k} \text{ is even,}$$

$$\mathrm{wt}(f_{n,s}) = 2^{n-1}, \qquad \mathrm{NL}(f_{n,s}) = 2^{n-1} - 2^{\frac{n+k}{2}-1}, \quad \text{otherwise.}$$

Proof. Suppose $\tau_i = (j, \rho_s(j), \ldots, \rho_s^{t-1}(j))$. The length t of τ_i is the smallest positive integer satisfying $\rho_s^t(j) = j$. Referring to the formula (1), it is equivalent to the condition $(s-1)t \equiv 0 \pmod n$, which shows that the length is independent of the choices of τ_i. Moreover, this also implies that the length t is equal to $\frac{n}{\gcd(n,s-1)}$. Note that the number of cycles k should satisfy $n = kt$.

As stated before, a cycle $\tau_i = (j, \rho_s(j), \ldots, \rho_s^{t-1}(j))$ determines a function $f_{\tau_i} := x_j x_{\rho_s(j)} + x_{\rho_s(j)} x_{\rho_s^2(j)} + \cdots + x_{\rho_s^{t-1}(j)} x_j$. By reindexing the variables of f_{τ_i} as $x_j \to x_1, x_{\rho_s(j)} \to x_2, \ldots$, it is equivalent to $f_{t,2}$. Therefore, we have $f_{n,s} \equiv f_{t,2}^{(1)} + \cdots + f_{t,2}^{(k)}$, where $f_{t,2}^{(i)}$ is derived from τ_i. Applying Lemma 7 to each of $f_{t,2}^{(i)}$ results in, for even t, $f_{t,2}^{(i)} \equiv x_1^{(i)} x_2^{(i)} + \cdots + x_{t-3}^{(i)} x_{t-2}^{(i)}$, and for odd t, $f_{t,2}^{(i)} \equiv x_1^{(i)} x_2^{(i)} + \cdots + x_{t-2}^{(i)} x_{t-1}^{(i)} + x_t^{(i)}$, where the superscripts are used to distinguish which variable belongs to which subfunction.

Hence, for even t, we have $f_{n,s} \equiv \sum_{i=1}^{k} \sum_{j=1}^{\frac{t}{2}-1} x_{2j-1}^{(i)} x_{2j}^{(i)}$. Note that this equivalent function has $k(\frac{t}{2} - 1) = \frac{n}{2} - k$ terms and $2k$ free variables. Applying Lemma 5 to this function yields $\mathrm{wt}(f_{n,s}) = \mathrm{NL}(f_{n,s}) = 2^{n-1} - 2^{n-(\frac{n}{2}-k)-1} = 2^{n-1} - 2^{\frac{n}{2}+k-1}$.

For odd t, we have $f_{n,s} \equiv \sum_{i=1}^{k} \left(\sum_{j=1}^{\frac{t-1}{2}} x_{2j-1}^{(i)} x_{2j}^{(i)} + x_t^{(i)} \right)$. Note that this equivalent function consists of $k\frac{t-1}{2} = \frac{n-k}{2}$ quadratic terms and k linear terms (n and k have the same parity). Applying Lemma 5 again, this function is balanced, and the nonlinearity is $2^{n-1} - 2^{n-\frac{n-k}{2}-1} = 2^{n-1} - 2^{\frac{n+k}{2}-1}$. □

Example 9. Consider the function $f_{12,4}$. The associated permutation $\rho_4 = \begin{pmatrix} 1 & 2 & \cdots & 12 \\ 4 & 5 & \cdots & 3 \end{pmatrix}$ has the cycle decomposition of $(1, 4, 7, 10)(2, 5, 8, 11)(3, 6, 9, 12)$. Hence, the length of cycles is 4 and the number of cycle is 3. Thus, $\mathrm{wt}(f_{12,4}) = \mathrm{NL}(f_{12,4}) = 2^{11} - 2^8 = 1792$.

Consider the function $f_{14,7}$. The associated permutation $\rho_7 = \begin{pmatrix} 1 & 2 & \cdots & 14 \\ 7 & 8 & \cdots & 6 \end{pmatrix}$ has the cycle decomposition of $(1, 7, 13, 5, 11, 3, 9)(2, 8, 14, 6, 12, 4, 10)$. Hence, the length of cycles is 7 and there are only two cycles. Thus, $f_{14,7}$ is balanced and $\mathrm{NL}(f_{14,7}) = 2^{13} - 2^7 = 8064$.

Remark 10. In view of Theorem 8, we can immediately notice that when n is odd, $f_{n,s}$ is balanced regardless of s. We also mention that the function $f_{n,s}$ is bent exactly when n is even and $s = \frac{n}{2} + 1$, which is in the class of Maiorana–McFarland functions.

Remark 11. The function $g_{n,r} := x_0 x_r + x_1 x_{r+1} + \cdots + x_{n-1} x_{r-1}$ where $r = s - 1$, is equivalent to $f_{n,s}$. It is associated with the permutation σ_r defined by $\sigma_r(i) = i + r \pmod n$. Clearly, ρ_s and σ_r have the same cycle structure. The orbit of r under σ_r is a cyclic subgroup of $\mathbb{Z}_n$, whose order is given by $\frac{n}{\gcd(n,r)}$.

6. Conclusion

In this paper, we characterized the exact weight and nonlinearity of $f_{n,s}$. By analyzing the naturally associated permutation of $f_{n,s}$, we showed that both values are directly connected to the cycle structure of the permutation. It would be interesting to examine whether the method applies to more general types of quadratic rotation symmetric functions which contain multiple orbits, or to cubic functions. We also expect that, by analyzing the equivalence transform in Lemma 7, other cryptographic properties of $f_{n,s}$ might be revealed.

Acknowledgements

The authors would like to express their appreciation to the anonymous reviewers for their valuable comments and suggestions.

References

[1] C. Carlet, Boolean functions for cryptography and error correcting codes, in: Y. Crama, P. Hammer, (Eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, U.K. (in press). Available online http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html.
[2] T.W. Cusick, P. Stanica, Fast evaluation, weights and nonlinearity of rotation-symmetric functions, Discrete Mathematics 258 (2002) 289–301.
[3] S. Kavut, S. Maitra, M.D. Yücel, Search for Boolean functions with excellent profiles in the rotation symmetric class, IEEE Transactions on Information Theory 53 (5) (2007) 1743–1751.
[4] F.J. MacWilliams, N.J. Sloane, The Theory of Error-Correcting Codes, North Holland, Amsterdam, 1977.
[5] Q. Meng, H. Zhang, M. Yang, J. Cui, On the degree of homogeneous bent functions, Discrete Applied Mathematics 155 (2007) 665–669.
[6] J. Pieprzyk, C.X. Qu, Fast hashing and rotation-symmetric functions, Journal of Universal Computer Science 5 (1) (1999) 20–31.
[7] P. Stanica, S. Maitra, Rotation symmetric functions—Count and cryptographic properties, Discrete Applied Mathematics (2007) doi:10.1016/j.dam.2007.04.029.
[8] P. Stanica, S. Maitra, Rotation symmetric Boolean functions — Count and cryptographic properties, Discrete Applied Mathematics 156 (2008) 1567–1580.
[9] T. Xia, J. Seberry, J. Pieprzyk, C. Charnes, Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$, Discrete Applied Mathematics 142 (2004) 127–132.